INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-29 14:01 UTC

EKZ Infostealer Exploits FortiClient EMS Authentication Bypass (CVE-2026-35616)

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0236
Type	CVE Vulnerability
CVE ID	CVE-2026-35616
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.4117 (97th percentile)
Affected Products	Fortinet FortiClient EMS 7.4.5, 7.4.6; FortiGate IPsec/VPN infrastructure
Published	2026-05-28T13:25:43
Discovery Source	Rss

Executive Summary

A critical authentication bypass vulnerability in Fortinet FortiClient Enterprise Management Server (versions 7.4.5 and 7.4.6) is being actively exploited to deliver EKZ, a previously undocumented infostealer. EKZ harvests browser-saved credentials, session cookies, and payment card data by disguising itself as a legitimate Fortinet software update pushed through VPN scripting workflows. Organizations running internet-exposed FortiClient EMS instances face immediate risk of credential theft and session hijacking that could enable broader network compromise.

Technical Analysis

CVE-2026-35616 is a critical authentication bypass (CVSS 9.5) affecting Fortinet FortiClient EMS versions 7.4.5 and 7.4.6, rooted in CWE-306 (Missing Authentication for Critical Function) and CWE-284 (Improper Access Control). Threat actors exploit the internet-exposed EMS management interface (T1190) to inject EKZ, a novel infostealer, via FortiClient VPN scripting workflows, abusing the legitimate software update delivery mechanism (T1036.005, T1195, T1059.001, T1059.003). EKZ collects browser credentials (T1555.003, T1555), session cookies (T1539), and payment card data, exfiltrates via C2 (T1041), and wipes local artifacts post-execution (T1070.004). Persistence may be achieved through account manipulation (T1078, T1098) and authentication modification (T1556). Approximately 2,000 EMS instances are estimated to be internet-exposed. EPSS score is 0.4117 (97.5th percentile), indicating high exploitation probability relative to other CVEs. The item data marks cisa_kev as false; if recent sources claim CISA KEV inclusion, cross-validate against the live CISA KEV catalog

(https://www.cisa.gov/known-exploited-vulnerabilities) and NVD entry before acting on that claim, as data may be stale. Fortinet PSIRT advisories are published at https://www.fortiguard.com/psirt; confirm patch availability and version guidance directly from Fortinet before applying fixes. Attribution remains unconfirmed.

Action Checklist

1. Containment: Immediately identify all FortiClient EMS instances running versions 7.4.5 or 7.4.6 using your asset inventory (CIS 1.1). Block internet-facing access to EMS management interfaces at the perimeter firewall (CIS 4.4, NIST AC-17). If internet exposure cannot be confirmed safe, isolate the EMS server from the network pending patching. Verify the confirmed safe patch version from Fortinet PSIRT (https://www.fortiguard.com/psirt) before deployment; do not assume any version is safe without explicit vendor confirmation.

2. Detection: Ensure audit logging is enabled per NIST AU-2 and AU-12 before hunting; gaps in logging coverage are themselves a finding and should be remediated in parallel (CIS 8.2). Then query EDR and SIEM for FortiClient VPN scripting process trees spawning unexpected child processes (T1059.001, T1059.003). Review FortiClient EMS logs for unauthenticated API calls or session anomalies. Search endpoint logs for processes masquerading as Fortinet update binaries from non-standard paths (T1036.005). Hunt for outbound connections from EMS hosts to unknown external IPs following VPN script execution (T1041). Review browser credential store access events on hosts managed by affected EMS instances (T1555.003, T1539).

3. Eradication: Apply the Fortinet-issued patch for CVE-2026-35616 as published in the FortiGuard PSIRT advisory. Until a patch is confirmed available and applied, enforce network-level controls blocking unauthenticated access to EMS (NIST AC-3, AC-6). Audit and remove any scripts or binaries delivered via FortiClient VPN scripting workflows that are not documented in your change management log or explicitly approved by Fortinet. Rotate all credentials and session tokens on systems managed by or connected through affected EMS instances (D3-CRO). Disable or remove unauthorized accounts created during the exploitation window (NIST AC-2).

4. Recovery: After patching, verify EMS is running the confirmed safe version. Re-enable network access incrementally with monitoring active. Validate that no EKZ artifacts persist: check for scheduled tasks, startup entries, and modified authentication configurations (D3-SICA, D3-SFA, T1556). Force re-authentication for all VPN and EMS-managed sessions (NIST IA, session controls, AC-12). Monitor outbound traffic from previously affected hosts for 30 days for residual C2 activity (NIST SI-4, AU-6).

5. Post-Incident: Conduct a lessons-learned review against NIST IR controls. Assess why internet-exposed EMS management interfaces were reachable, close the gap with network segmentation and least-privilege access (NIST AC-6, AC-4, CIS 4.4). Implement MFA for all EMS administrative access (CIS 6.5, D3-MFA). Establish a formal Fortinet advisory monitoring process so future PSIRT advisories trigger immediate triage. Review VPN scripting workflow permissions to prevent abuse as a delivery vector (NIST CM controls, CIS 4.6).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership, legal counsel, and privacy/compliance officers immediately if forensic analysis confirms EKZ successfully harvested credentials or session cookies from EMS-managed endpoints, as exfiltrated browser-saved payment card data or PII may trigger PCI-DSS breach notification obligations and state/federal privacy law reporting requirements.
Recovery Notes	After applying the CVE-2026-35616 patch confirmed in the FortiGuard PSIRT advisory, verify EMS integrity by comparing the installed binary hashes against Fortinet-published values before restoring internet-facing access — do not rely solely on version strings, as EKZ's masquerade mechanism targets Fortinet binary naming conventions. Maintain enhanced outbound traffic monitoring on the EMS host and all endpoints that connected through the affected EMS for a minimum of 30 days, specifically watching for low-frequency HTTPS beaconing to external IPs first observed during the exploitation window, as EKZ may stage exfiltration asynchronously after initial credential harvest. Treat all credentials and session tokens that transited the affected EMS as fully compromised regardless of whether forensic evidence of access is confirmed, given the authentication bypass nature of CVE-2026-35616.
Forensic Artifacts	FortiClient EMS Apache access logs (`C:\Program Files\Fortinet\FortiClientEMS\logs\apache\access.log`) — CVE-2026-35616 authentication bypass will produce HTTP 200 success responses on EMS REST API endpoints from requests lacking valid session tokens; filter for unauthenticated calls to EMS management API paths in the exploitation window | Windows Prefetch files (`C:\Windows\Prefetch\`) on the EMS host and managed endpoints for executables masquerading as Fortinet update binaries (e.g., `FORTICLIENTUPDATE.EXE-*.pf`, `FORTIGUARD*.EXE-*.pf`) executed from `%TEMP%`, `%APPDATA%`, or `%LOCALAPPDATA%` paths — EKZ disguises itself as a legitimate FortiClient update pushed via VPN scripting, making non-standard execution paths a primary indicator | Browser credential store SQLite databases on managed endpoints (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data`, `%APPDATA%\Mozilla\Firefox\Profiles\*.default\key4.db`, `%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data`) — examine file system last-accessed timestamps and Windows Event ID 4663 Object Access events to identify EKZ credential harvesting activity on hosts that received VPN scripts from the affected EMS | FortiClient EMS endpoint management database (MSSQL or embedded DB at the EMS data directory) — query the script deployment history table for all scripts pushed to managed endpoints during and 72 hours prior to the exploitation window, capturing script names, hashes, target endpoint lists, and execution timestamps to scope EKZ delivery across the managed device population | Windows Security Event Log Event ID 4720 (User Account Created) and 4732 (Member Added to Security-Enabled Global Group) on the EMS host and domain controllers, covering the full exploitation window — threat actors exploiting authentication bypass vulnerabilities frequently create or elevate backdoor accounts as a persistence mechanism before or alongside infostealer deployment

Per-Action IR Details

Containment — Immediately identify all FortiClient EMS instances running versions 7.4.5 or 7.4.6 using your asset inventory (CIS 1.1). Block internet-facing access to EMS management interfaces at the perimeter firewall (CIS 4.4, NIST AC-17). If internet exposure cannot be confirmed safe, isolate the EMS server from the network pending patching. Check FortiGuard PSIRT (https://www.fortiguard.com/psirt) for the vendor-confirmed patch version — do not assume a version is safe without explicit vendor confirmation.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), NIST IR-4 (Incident Handling), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without enterprise asset management tooling, run: `nmap -p 8013,8014 --open -sV` to identify internet-exposed FortiClient EMS management ports (default 8013/TCP for EMS console). Cross-reference with `netstat -an | findstr ':8013'` on candidate hosts. Apply immediate perimeter block via firewall CLI (e.g., iptables: `iptables -I INPUT -p tcp --dport 8013 -j DROP`) or equivalent ACL on edge router. Document all identified EMS instances in a flat spreadsheet before isolation to track remediation scope.

Evidence: Before isolating the EMS server, capture: (1) full netstat output showing active connections to EMS management ports 8013/8014 — document all external source IPs; (2) FortiClient EMS Apache/IIS access logs at `C:\Program Files\Fortinet\FortiClientEMS\logs\` showing unauthenticated or anomalous API requests against the EMS REST API endpoints; (3) Windows Security Event Log Event ID 4624/4625 on the EMS host covering the 72-hour window prior to isolation, filtered for logon type 3 (network) from external IPs; (4) running process list (`tasklist /v`) and active network connections (`netstat -bno`) at time of isolation to capture any in-flight EKZ staging activity.

Detection — Query EDR and SIEM for FortiClient VPN scripting process trees spawning unexpected child processes (T1059.001, T1059.003). Review FortiClient EMS logs for unauthenticated API calls or session anomalies. Search endpoint logs for processes masquerading as Fortinet update binaries from non-standard paths (T1036.005). Hunt for outbound connections from EMS hosts to unknown external IPs following VPN script execution (T1041). Review browser credential store access events on hosts managed by affected EMS instances (T1555.003, T1539). Enable or verify audit logging per NIST AU-2, AU-12, and CIS 8.2 before hunting — gaps in logging are themselves a finding.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without EDR/SIEM: (1) Deploy Sysmon with SwiftOnSecurity config — specifically ensure Event ID 1 (Process Create) captures ParentImage to catch `FortiESNAC.exe` or `FortiClientEMS.exe` spawning `cmd.exe`, `powershell.exe`, or `wscript.exe`; (2) Run this PowerShell to hunt masquerading Fortinet binaries: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688} | Where-Object {$_.Message -like '*fortinet*' -or $_.Message -like '*forticlient*'} | Select-Object TimeCreated, Message | Export-Csv fortinet_procs.csv`; (3) Use Wireshark or `netsh trace start capture=yes` to capture outbound traffic from EMS host for C2 beacon analysis; (4) Check browser credential stores manually: `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` and Firefox `key4.db` for unexpected access timestamps using `dir /tc` on Windows.

Evidence: Collect before hunting to preserve original state: (1) FortiClient EMS application logs at `C:\Program Files\Fortinet\FortiClientEMS\logs\apache\access.log` — filter for HTTP 200 responses on unauthenticated endpoints (CVE-2026-35616 authentication bypass would produce successful responses to API calls lacking valid session tokens); (2) Windows Sysmon Event ID 3 (Network Connection) from the EMS host showing outbound connections post-script-execution — EKZ exfiltrates via HTTPS to external C2, so flag any new external IPs contacted by FortiClient-related processes; (3) FortiClient VPN script execution logs showing the specific script name and hash that delivered EKZ disguised as a Fortinet update binary; (4) Windows Event ID 4663 (Object Access) on browser profile directories (`Login Data`, `Cookies`, `Web Data`) on managed endpoints, indicating EKZ credential harvesting activity; (5) Prefetch files at `C:\Windows\Prefetch\` for any executable masquerading as a Fortinet update (e.g., `FORTICLIENTUPDATE.EXE-*.pf`) executed from non-standard paths such as `%TEMP%` or `%APPDATA%`.

Eradication — Apply the Fortinet-issued patch for CVE-2026-35616 as published in the FortiGuard PSIRT advisory. Until a patch is confirmed available and applied, enforce network-level controls blocking unauthenticated access to EMS (NIST AC-3, AC-6). Remove any unauthorized scripts or binaries delivered via FortiClient VPN scripting workflows. Rotate all credentials and session tokens on systems managed by or connected through affected EMS instances (D3-CRO). Disable or remove unauthorized accounts created during the exploitation window (NIST AC-2).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without automated patch management: (1) Download the CVE-2026-35616 patch directly from FortiGuard PSIRT and verify the binary hash against the published SHA256 before applying — do not pull from any mirror or CDN; (2) Audit FortiClient EMS VPN scripting workflows via the EMS console under `Endpoint Policy > Script Deployment` — export the full script list and diff against your last known-good configuration baseline; (3) Hunt for EKZ persistence without EDR using: `schtasks /query /fo LIST /v | findstr /i fortinet` and `reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` on the EMS host and all managed endpoints that connected during the exploitation window; (4) For credential rotation without a PAM tool, use a PowerShell loop to force AD password resets for all accounts that authenticated through the affected EMS: `Get-ADUser -Filter * | Where-Object {$_.LastLogonDate -gt (Get-Date).AddDays(-30)} | Set-ADAccountPassword -Reset`.

Evidence: Before patching or removing artifacts, capture: (1) A full disk image or at minimum a forensic copy of `C:\Program Files\Fortinet\FortiClientEMS\` and the EMS database (`FortiClientEMS.db` or equivalent SQL instance) to preserve pre-patch state for post-incident analysis; (2) Hash and preserve all scripts found in FortiClient VPN scripting workflow directories — EKZ was delivered as a masquerading update binary, so capture any `.exe`, `.ps1`, or `.bat` files dropped in `%TEMP%`, `%APPDATA%\Fortinet\`, or FortiClient installation subdirectories during the exploitation window; (3) Windows Event ID 4720 (Account Created) and 4732 (Account Added to Security-Enabled Group) from the EMS host and domain controllers covering the exploitation window, to identify backdoor accounts created by the threat actor; (4) Export full FortiClient EMS account list from the EMS console before disabling accounts, to document attacker-created entries.

Recovery — After patching, verify EMS is running the confirmed safe version. Re-enable network access incrementally with monitoring active. Validate that no EKZ artifacts persist: check for scheduled tasks, startup entries, and modified authentication configurations (D3-SICA, D3-SFA, T1556). Force re-authentication for all VPN and EMS-managed sessions (NIST IA — session controls, AC-12). Monitor outbound traffic from previously affected hosts for 30 days for residual C2 activity (NIST SI-4, AU-6).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-12 (Session Termination), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST IA-2 (Identification and Authentication — Organizational Users), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Without enterprise monitoring during recovery: (1) Verify patched EMS version via FortiClient EMS console `Help > About` or CLI: `diagnose sys version` — confirm it matches the PSIRT-confirmed safe build exactly; (2) Use Autoruns (Sysinternals) on the EMS host and all managed endpoints that connected during exploitation to enumerate all persistence mechanisms — specifically check `ScheduledTasks`, `Services`, `Winlogon`, and `AppInit_DLLs` tabs for EKZ residue masquerading as Fortinet components; (3) Deploy a YARA rule targeting EKZ's masquerade pattern (Fortinet-named executables in non-standard paths) using `yara64.exe ekz_rule.yar C:\ -r`; (4) Establish a 30-day Wireshark or `netsh trace` monitoring window on the EMS host's egress interface, filtering for HTTPS connections to new external IPs not present in the pre-incident baseline.

Evidence: During recovery verification, capture: (1) FortiClient EMS version string and build number post-patch, documented with timestamp and analyst name, for change management records; (2) Autoruns or `schtasks /query` output from all previously managed endpoints showing clean state — retain as a post-remediation baseline; (3) NetFlow or firewall connection logs showing outbound traffic patterns from the EMS host and managed endpoints for the 30-day monitoring window — EKZ C2 beaconing may use jitter to evade detection, so look for low-volume HTTPS connections to the same external IP on irregular intervals; (4) Forced re-authentication events from FortiGate VPN logs confirming all prior sessions were invalidated.

Post-Incident — Conduct a lessons-learned review against NIST IR controls. Assess why internet-exposed EMS management interfaces were reachable — close the gap with network segmentation and least-privilege access (NIST AC-6, AC-4, CIS 4.4). Implement MFA for all EMS administrative access (CIS 6.5, D3-MFA). Establish a formal Fortinet advisory monitoring process so future PSIRT advisories trigger immediate triage.

Review VPN scripting workflow permissions to prevent abuse as a delivery vector (NIST CM controls, CIS 4.6).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST CM-2 (Baseline Configuration), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For a resource-constrained team: (1) Conduct a 1-hour structured lessons-learned using the NIST 800-61r3 §4 question set — specifically document: how long EMS was internet-exposed, when CVE-2026-35616 was published versus when patching began, and whether VPN script delivery permissions had ever been reviewed; (2) Harden FortiClient EMS VPN scripting by auditing the script deployment policy — restrict script execution permissions to named admin accounts only and log all script push events; (3) Subscribe to FortiGuard PSIRT RSS feed (`https://www.fortiguard.com/rss/psirt.xml`) and configure a free RSS-to-email alert so future critical advisories for FortiClient EMS trigger same-day triage; (4) Without a commercial MFA solution, enable Fortinet's built-in two-factor authentication for EMS admin accounts using FortiToken Mobile (free tier available) as documented in the FortiClient EMS Administration Guide.

Evidence: For the post-incident report, compile: (1) Timeline reconstruction from FortiClient EMS access logs and Windows Security Event Logs showing first unauthenticated API call (initial exploitation), first EKZ binary execution, first credential store access, and first C2 outbound connection — this establishes attacker dwell time; (2) Full list of managed endpoints that received FortiClient VPN scripts during the exploitation window, with the specific script hashes, to scope potential EKZ delivery to the full managed device population; (3) Network diagram annotated to show why EMS port 8013/8014 was reachable from the internet — document the specific firewall rule or misconfiguration that permitted exposure, as this drives the segmentation remediation; (4) Credential exposure inventory listing all accounts that authenticated through the affected EMS during the exploitation window, for breach notification scope assessment if PII or regulated data was accessible via those credentials.

Detection Guidance

Hunt in SIEM and EDR for: (1) FortiClient VPN scripting engine (FCConfig.exe or equivalent) spawning cmd.exe, PowerShell, or wscript as child processes (T1059.001, T1059.003). (2) Processes with Fortinet-themed names executing from non-standard directories such as %TEMP%, %APPDATA%, or user profile paths, a masquerading indicator (T1036.005). (3) Access to browser credential stores (Login Data, Cookies databases for Chrome/Edge/Firefox) by non-browser processes (T1555.003, T1539). (4) Outbound HTTPS or DNS traffic from EMS management hosts to external IPs not in your known-good baseline, particularly following script execution events (T1041). (5) File deletion events following data access, EKZ removes local artifacts post-exfiltration (T1070.004). (6) Authentication events against FortiClient EMS APIs that lack a preceding valid credential exchange (CWE-306 exploitation pattern). Use NIST AU-6 review cadence; ensure AU-3 fields (what, when, where, who, outcome) are present in all relevant log sources. Note: No confirmed IOC hashes or C2 infrastructure were available in sources at time of publication. Conduct behavioral and process-tree hunting (indicators 1-6 above) in lieu of hash-based detection; behavioral indicators are more reliable for novel malware such as EKZ.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available at time of publication`	Source reporting did not include verified hashes, C2 IPs, or domains for EKZ. Cross-validate with Arctic Wolf blog and NVD entry for updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1555.003** — Credentials from Web Browsers
- **T1539** — Steal Web Session Cookie
- **T1059.003** — Windows Command Shell
- **T1556** — Modify Authentication Process
- **T1195** — Supply Chain Compromise
- **T1041** — Exfiltration Over C2 Channel
- **T1566** — Phishing
- **T1059.001** — PowerShell
- **T1078** — Valid Accounts
- **T1555** — Credentials from Password Stores
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1098** — Account Manipulation
- **T1190** — Exploit Public-Facing Application
- **T1070.004** — File Deletion

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-7** — Software, Firmware, and Information Integrity
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection

- **AC-2** — Account Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-3** — Access Enforcement
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1555.003	Credentials from Web Browsers	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1059.003	Windows Command Shell	Execution
T1556	Modify Authentication Process	Credential-Access
T1195	Supply Chain Compromise	Initial-Access

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1566	Phishing	Initial-Access
T1059.001	PowerShell	Execution
T1078	Valid Accounts	Defense-Evasion
T1555	Credentials from Password Stores	Credential-Access
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1098	Account Manipulation	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1070.004	File Deletion	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/hackers-exploit-fort...	T3
CVE-2026-35616 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-35616	T1
FortiClient EMS Exploited via CVE-2026-35616 to Deliver ...	https://arcticwolf.com/resources/blog/forticlient-ems-exploited-via...	T3
Fortinet CVE-2026-35616 Actively Exploited as Zero Day	https://www.reddit.com/r/cybersecurity/comments/1scm5bc/fortinet_cv...	T3
Fortinet FortiClient EMS vulnerability: CVE-2026-35616	https://www.runzero.com/blog/fortinet-forticlient-ems/	T3

Generated 2026-05-29 14:01 UTC by TJS Security Command Center